

Nonbinary Quantum Codes from Two-Point Divisors on Hermitian Curves

Martianus Frederic Ezerman and Radoslav Kirov

Abstract—Sarvepalli and Klappenecker showed how classical one-point codes on the Hermitian curve can be used to construct quantum codes. Homma and Kim determined the parameters of a larger family of codes, the two-point codes. In quantum error-correction, the observed presence of asymmetry in some quantum channels led to the study of asymmetric quantum codes (AQECCs) where we no longer assume that the different types of errors are equiprobable. This paper considers quantum codes constructed from the two-point codes. In the asymmetric case, we show strict improvements over all possible finite fields for a range of designed distances. We produce large dimension pure AQECC and small dimension impure AQECC that have better parameters than AQECC from one-point codes. Numerical results for the Hermitian curves over \mathbb{F}_{16} and \mathbb{F}_{64} are used to illustrate the gain.

Index Terms—Algebraic geometric codes, Hermitian curve, quantum codes, asymmetric quantum codes

I. INTRODUCTION

The term *quantum codes* is a shorthand for quantum error-correcting codes. Quantum codes have been garnering a lot of interest since they protect information-carrying quantum states against decoherence and play an important part in making fault-tolerant quantum computation possible. Quantum codes can be distinguished into *pure* and *impure* (or *degenerate*). The pure ones are usually easier to implement due to their simpler decoding process while the degenerate ones give us better error-detecting capabilities.

In the nonbinary cases, a firm connection between classical error-correcting codes and quantum codes is well-established. We can construct quantum codes from classical codes by using the stabilizer formalism [7]. The resulting quantum codes are called *stabilizer codes*. A subclass of these codes can be derived by using the CSS method.

The class of Hermitian codes is known to have excellent parameters. They are easy to describe, to encode and to decode. The most studied Hermitian codes are the one-point codes. Vector spaces of functions that correspond to two-point divisors were first studied in [8]. A complete description of the minimum distances of all two-point Hermitian codes is given in [6]. Further results discussed in [6], [2], [9], and [4] improve our understanding of these codes. Two-point codes have better parameters than one-point codes, while maintaining their ease of construction.

This paper is organized as follows. Section II contains three subsections. They discuss, respectively, Hermitian

codes, quantum codes, and three relevant construction methods that will be needed to derive quantum codes. Section III establishes the parameters of quantum codes derived from two-point Hermitian codes and compare them with the corresponding parameters of quantum codes from one-point codes. Using coset bounds we can construct excellent impure AQECCs of small dimension. This fact and related results are contained in Section IV.

II. PRELIMINARIES

Let \mathbb{F}_q denote the finite field of cardinality $q = p^m$ for a prime p and $m \in \mathbb{N}$. The trace mapping $\text{Tr} : \mathbb{F}_q \rightarrow \mathbb{F}_p$ is given by $\text{Tr}(\beta) = \beta + \beta^p + \beta^{p^2} + \dots + \beta^{p^{m-1}}$. Given any two distinct (nonempty) subsets C and D of \mathbb{F}_q^n , let the notation $\text{wt}(C \setminus D)$ denote $\min\{\text{wt}(\mathbf{u}) : \mathbf{u} \in (C \setminus D), \mathbf{u} \neq \mathbf{0}\}$ with $\text{wt}(\mathbf{u})$ denoting the Hamming weight of \mathbf{u} .

For $\mathbf{u} = (u_1, u_2, \dots, u_n), \mathbf{v} = (v_1, v_2, \dots, v_n) \in \mathbb{F}_q^n$,

- 1) $\langle \mathbf{u}, \mathbf{v} \rangle_E = \sum_{i=1}^n u_i v_i$ is the *Euclidean inner product* of \mathbf{u} and \mathbf{v} .
- 2) If \mathbb{F}_q is a quadratic extension of $\mathbb{F}_{e=p^l}$, then $\langle \mathbf{u}, \mathbf{v} \rangle_H = \sum_{i=1}^n u_i v_i^e$ is the *Hermitian inner product* of \mathbf{u} and \mathbf{v} .

Let C be an $[n, k, d]_q$ -code. Let $*$ represent either the Euclidean or the Hermitian inner product, the *dual code* $C^{\perp*}$ of C is given by

$$C^{\perp*} := \{\mathbf{u} \in \mathbb{F}_q^n : \langle \mathbf{u}, \mathbf{v} \rangle_* = 0 \text{ for all } \mathbf{v} \in C\}$$

while the dual distance $d^{\perp*}$ is defined to be $d(C^{\perp*})$.

A *monomial matrix* M is a square matrix over \mathbb{F}_q with exactly one nonzero entry in each row and each column. Such a matrix can be written as TP or PT' where T and T' are diagonal matrices and P is a permutation matrix. Two codes C and C' are said to be (*monomially*) *equivalent* if there is a monomial matrix M such that $G' = MG$, for the corresponding generator matrices G and G' . Equivalent codes have the same parameters.

A. Hermitian Codes

We recall Goppa's general construction of codes from curves. Let X/\mathbb{F}_q be an algebraic curve (absolutely irreducible, smooth, projective) of genus g over \mathbb{F}_q . Let $\mathbb{F}_q(X)$ be the function field of X/\mathbb{F}_q and $\Omega(X)$ be the module of rational differentials of X/\mathbb{F}_q .

Given a divisor E on X defined over \mathbb{F}_q , let $L(E) = \{f \in \mathbb{F}_q(X) \setminus \{0\} : (f) + E \geq 0\} \cup \{0\}$, and let $\Omega(E) = \{\omega \in \Omega(X) \setminus \{0\} : (\omega) \geq E\} \cup \{0\}$. Let K represent

the canonical divisor class. For n distinct rational points P_1, \dots, P_n on X/\mathbb{F}_q and for disjoint divisors $D = P_1 + \dots + P_n$ and G , the geometric Goppa codes $C_L(D, G)$ and $C_\Omega(D, G)$ are defined as the images of the maps

$$\begin{aligned}\alpha_L : L(G) &\longrightarrow \mathbb{F}^n, f \mapsto (f(P_1), \dots, f(P_n)). \\ \alpha_\Omega : \Omega(G - D) &\longrightarrow \mathbb{F}^n, \\ \omega &\mapsto (\text{Res}_{P_1}(\omega), \dots, \text{Res}_{P_n}(\omega)).\end{aligned}$$

A consequence of the Residue Theorem for function fields is that $C_L(D, G)^{\perp_E} = C_\Omega(D, G)$ [13, Theorem 2.2.8]. Moreover, the residue construction can be represented as an evaluation.

Lemma 2.1 ([13, Proposition 2.2.10]): Let ν be a differential with simple poles and residue 1 at the points of D . Then

$$C_L(D, G)^{\perp_E} = C_\Omega(D, G) = C_L(D, D - G + (\nu)).$$

In this paper we only consider the Hermitian curve, which is the smooth projective curve over \mathbb{F}_{q^2} with affine equation $y^q + y = x^{q+1}$. It achieves the Hasse-Weil bound with $q^3 + 1$ rational points and genus $g = q(q-1)/2$.

Classical two-point codes are the codes $C_L(D, G)$ and $C_\Omega(D, G)$ with Goppa divisor $G = iP + jQ$. To construct them, we fix two distinct rational points P and Q . The standard choice is to let P be the point at infinity (the common pole of x and y) and Q be the origin (the common zero of x and y). The equivalent divisors $(q+1)P \sim (q+1)Q$ belong to the hyperplane divisor class H with respect to the model above. The divisor sum R of all $q^3 + 1$ rational points belongs to the divisor class $(q^2 - q + 1)H$ and the canonical divisor class $K = (q-2)H$. See [14], [12], [13, Section 8.3] and [15, Section 4.4.3] for the details.

Henceforth, we fix the divisor D to be $R - P - Q$, making the length of the constructed codes $q^3 - 1$. The two-point codes are one coordinate shorter than the one-point codes. In order to compare the two families, we shorten one-point codes. Since the automorphism group of a one-point code acts transitively on the set of coordinates [13, Remark 8.3.6], the choice of coordinate is non-essential. Thus the minimum distance of the code is preserved under shortening. This feature makes it easy to compare two-point codes of length $q^3 - 1$ with the shortened one-point codes of equal dimension.

It is known that the Euclidean duals of one-point codes are also one-point codes. We extend this property to two-point codes.

Proposition 2.2: If $D = R - P - Q$, then

$$\begin{aligned}C_L(D, iP - jQ)^{\perp_E} = \\ C_L(D, (q^3 + q^2 - q - 2 - i)P + (j - 1)Q).\end{aligned}$$

Proof: Following the proof for one-point codes in [13, Proposition 8.3.2], we select $\nu = dt/t$, with $t = x^{q^2} - x$, and apply Lemma 2.1. ■

Self-orthogonality property is important in some construction of quantum codes.

Corollary 2.3: If $D = R - P - Q$, $G = iP + jQ$ and $G' = i'P + j'Q$, then

$$C_L(D, G)^{\perp_E} \subseteq C_L(D, G')$$

if $q^3 + q^2 - q - 2 \leq i + i'$ and $-1 \leq j + j'$. The code $C_L(D, iP + jQ)$ is Euclidean self-orthogonal if $2i \leq q^3 + q^2 - q - 2$ and $j \leq 0$.

Equivalent divisors $G \sim \widehat{G}$ produce equivalent geometric Goppa codes $C(D, G)$ and $C(D, \widehat{G})$ under both maps α_L and α_Ω .

Due to the equivalence $(q+1)P \sim (q+1)Q$, every two-point code (using either construction) is uniquely equivalent to a code of the form $C_L(D, iP - jQ)$ with $0 \leq j \leq q$. We use this representation as a canonical one. Moreover, a particularly favorable feature of the Hermitian curves is that one can explicitly write a monomial basis for the Riemann-Roch space of a two-point divisor of that form.

Lemma 2.4 ([9]): Let $D = c(q+1)P - aP - bQ$, for $c \in \mathbb{Z}$, and for $0 \leq a, b \leq q$. The space $L(D)$ has a basis given by the monomials $x^i y^j$ where:

- 1) $0 \leq i \leq q$, $0 \leq j$, and $i + j \leq c$,
- 2) $a \leq i$ for $i + j = c$,
- 3) $b \leq i$ for $j = 0$.

The actual minimum distance of two-point codes was determined by Homma and Kim in [5, Th. 5.2 and Th. 6.1] for $n = 0$ and $n = q$, as well as in [6, Th. 1.3 and Th. 1.4] for $0 < n < q$. Using order bound techniques, Beelen in [2, Th. 17] gives lower bounds for the cases $\deg G > \deg K$ (i.e. for $m + n > (q-2)(q+1)$), and Park settles all cases in [9, Th. 3.3 and Th. 3.5]. Park moreover shows that the lower bounds are sharp and that they correspond to the actual minimum distance. In [4], Duursma and Kirov show that among all divisors $G = iP + jQ$ of a given degree, the optimal minimum distance is attained for a choice of the form $G = aP - 2Q$.

Proposition 2.5 ([4]): Let $G = K + B$ where B is a divisor such that $B \neq 0$, $\deg B \geq 0$ and $B = cH - aP - bQ$, for $0 \leq a \leq q$. If $D \cap \{P, Q\} = \emptyset$, then the two-point code $C_L(D, G)$ has dimension $\deg G - g + 1$ and dual distance

$$\mathbf{d}^{\perp_E} = \begin{cases} \deg B + \max(0, q - c) & \text{if } a = q, \text{ otherwise,} \\ \deg B + \max(0, q - c) + \max(0, a - c). \end{cases}$$

The corresponding one-point code of the same dimension has the same minimum distance if $a = q$, but $\max(0, q - c)$ less if otherwise.

Using Proposition 2.2, we can restate the result for the minimum distance of the evaluation codes.

Corollary 2.6: Let $0 \leq r \leq q(q+1)$, and let $1 \leq c$ and $0 \leq a \leq q$ be the unique numbers such that $r + q = c(q+1) - a$. The code $C_L(D, (q^3 - r + 1)P - 2Q)$ is

a $[q^3 - 1, k(r), d(r)]_{q^2}$ code where

$$k(r) = q^3 - q(q-1)/2 - r,$$

$$d(r) = \begin{cases} r + \max(0, q-c) & \text{if } a = q, \text{ otherwise,} \\ r + \max(0, q-c) + \max(0, a-c). \end{cases}$$

Note that the range for r can be extended, but outside the given range there are no improvements over one-point codes.

B. Quantum Codes

Let \mathbb{C} be the field of complex numbers and $\eta = e^{\frac{2\pi\sqrt{-1}}{p}} \in \mathbb{C}$. Let $V_n = (\mathbb{C}^q)^{\otimes n} = \mathbb{C}^{q^n}$ be the n th tensor product of \mathbb{C}^q . V_n has the following orthonormal basis

$$\{|\mathbf{c}\rangle = |c_1 c_2 \dots c_n\rangle : \mathbf{c} = (c_1, \dots, c_n) \in \mathbb{F}_q^n\}, \quad (1)$$

where $|c_1 c_2 \dots c_n\rangle$ abbreviates $|c_1\rangle \otimes |c_2\rangle \otimes \dots \otimes |c_n\rangle$.

For two quantum states $|\varphi\rangle$ and $|\psi\rangle$ in V_n with

$$|\varphi\rangle = \sum_{\mathbf{c} \in \mathbb{F}_q^n} \alpha(\mathbf{c})|\mathbf{c}\rangle \text{ and } |\psi\rangle = \sum_{\mathbf{c} \in \mathbb{F}_q^n} \beta(\mathbf{c})|\mathbf{c}\rangle,$$

where $\alpha(\mathbf{c}), \beta(\mathbf{c}) \in \mathbb{C}$, the inner product of $|\varphi\rangle$ and $|\psi\rangle$ is given by

$$\langle \varphi | \psi \rangle = \sum_{\mathbf{c} \in \mathbb{F}_q^n} \widetilde{\alpha(\mathbf{c})} \beta(\mathbf{c}) \in \mathbb{C},$$

where $\widetilde{\alpha(\mathbf{c})}$ is the complex conjugate of $\alpha(\mathbf{c})$. We say $|\varphi\rangle$ and $|\psi\rangle$ are *orthogonal* if $\langle \varphi | \psi \rangle = 0$.

Essentials on the standard mathematical error model of quantum error-correction can be found, for instance, in [1] and in [7] for the symmetric case and in [16] for the asymmetric case.

To define a quantum code Q , we need to consider the set of error operators that Q can handle. Let $\alpha, \beta \in \mathbb{F}_q$. The unitary operators $X(\alpha)$ and $Z(\beta)$ on \mathbb{C}^q are defined by

$$X(\alpha)|\varphi\rangle = |\varphi + \alpha\rangle \text{ and } Z(\beta)|\varphi\rangle = \eta^{\text{Tr}(\langle \beta, \varphi \rangle_{\mathbb{E}})}|\varphi\rangle. \quad (2)$$

Based on Equation (2), for $\mathbf{a} = (\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q^n$, we can write $X(\mathbf{a}) = X(\alpha_1) \otimes \dots \otimes X(\alpha_n)$ and $Z(\mathbf{a}) = Z(\alpha_1) \otimes \dots \otimes Z(\alpha_n)$ for the tensor product of n error operators. The set $\mathcal{E}_n := \{X(\mathbf{a})Z(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n\}$ is a nice error basis on V_n .

The error group G_n of order pq^{2n} is generated by the matrices in \mathcal{E}_n

$$G_n := \{\eta^c X(\mathbf{a})Z(\mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n, c \in \mathbb{F}_p\}.$$

Let $E = \eta^c X(\mathbf{a})Z(\mathbf{b}) \in G_n$. Then the *quantum weight* $\text{wt}_Q(E)$ of E is the number of coordinates such that $(\alpha_i, \beta_i) \neq (0, 0)$. The number of X -errors $\text{wt}_X(E)$ and the number of Z -errors $\text{wt}_Z(E)$ in the error operator E are given, respectively, by $\text{wt}(\mathbf{a})$ and $\text{wt}(\mathbf{b})$.

Definition 2.7: A q -ary quantum code of length n is a subspace Q of V_n with dimension $\mathcal{K} \geq 1$. A quantum code Q of dimension $\mathcal{K} \geq 2$ is said to detect

$d-1$ quantum digits of errors for $d \geq 1$ if, for every orthogonal pair $|\varphi\rangle$ and $|\psi\rangle$ in Q and every $E \in G_n$ with $\text{wt}_Q(E) \leq d-1$, $|\varphi\rangle$ and $E|\psi\rangle$ are orthogonal. In this case, we call Q a *symmetric* quantum code with parameters $((n, \mathcal{K}, d))_q$ or $[[n, k, d]]_q$, where $k = \log_q \mathcal{K}$. Such a quantum code is called *pure* if $|\varphi\rangle$ and $E|\psi\rangle$ are orthogonal for any (not necessarily orthogonal) $|\varphi\rangle$ and $|\psi\rangle$ in Q and any $E \in G_n$ with $1 \leq \text{wt}_Q(E) \leq d-1$. A quantum code Q with $\mathcal{K} = 1$ is assumed to be pure.

Let d_x and d_z be positive integers. A quantum code Q in V_n with dimension $\mathcal{K} \geq 2$ is called an *asymmetric quantum code* with parameters $((n, \mathcal{K}, d_z/d_x))_q$ or $[[n, k, d_z/d_x]]_q$, where $k = \log_q \mathcal{K}$, if Q detects d_x-1 quantum digits of X -errors and, at the same time, d_z-1 quantum digits of Z -errors. That is, if $\langle \varphi | \psi \rangle = 0$ for $|\varphi\rangle, |\psi\rangle \in Q$, then $|\varphi\rangle$ and $E|\psi\rangle$ are orthogonal for any $E \in G_n$ such that $\text{wt}_X(E) \leq d_x-1$ and $\text{wt}_Z(E) \leq d_z-1$. Such an asymmetric quantum code Q is called *pure* if $|\varphi\rangle$ and $E|\psi\rangle$ are orthogonal for any $|\varphi\rangle, |\psi\rangle \in Q$ and any $E \in G_n$ such that $1 \leq \text{wt}_X(E) \leq d_x-1$ or $1 \leq \text{wt}_Z(E) \leq d_z-1$. An asymmetric quantum code Q with $\mathcal{K} = 1$ is assumed to be pure.

Remark 2.8: An asymmetric quantum code with parameters $((n, \mathcal{K}, d/d))_q$ is a symmetric quantum code with parameters $((n, \mathcal{K}, d))_q$, but the converse is not true since, for $E \in G_n$ with $\text{wt}_X(E) \leq d-1$ and $\text{wt}_Z(E) \leq d-1$, $\text{wt}_Q(E)$ may be bigger than $d-1$.

C. Constructions of Quantum Codes from Classical Codes

It is well-known that quantum codes can be constructed from classical codes. We will use the following three constructions tailored to Hermitian codes.

Lemma 2.9: (CSS Construction)[7, Lem. 20] Let C_i be an $[n, k_i, d_i]_{q^2}$ -code for $i = 1, 2$. Let $C_1^{\perp_E} \subseteq C_2$. Then there exists a symmetric quantum code Q with parameters $[[n, k_1 + k_2 - n, \min\{\text{wt}(C_2 \setminus C_1^{\perp_E}), \text{wt}(C_1 \setminus C_2^{\perp_E})\}]]_{q^2}$ which is pure whenever $\min\{\text{wt}(C_2 \setminus C_1^{\perp_E}), \text{wt}(C_1 \setminus C_2^{\perp_E})\} = \min\{d_i\}$. If we have $C \subseteq C^{\perp_E}$ where C is an $[n, k, d]_{q^2}$ -code, then Q is an $[[n, n-2k, \text{wt}(C^{\perp_E} \setminus C)]]_{q^2}$ -code which is pure whenever $d^{\perp_E} = \text{wt}(C^{\perp_E} \setminus C)$.

If, instead of the Euclidean, we use the Hermitian inner product, we have the following construction of a q -ary quantum code from a Hermitian self-orthogonal code $C \subseteq \mathbb{F}_{q^2}^n$.

Lemma 2.10: [7, Cor. 19] Let C be an $[n, k, d]_{q^2}$ -code such that $C \subseteq C^{\perp_H}$. Then there exists a symmetric quantum code Q with parameters $[[n, n-2k, \text{wt}(C^{\perp_H} \setminus C)]]_{q^2}$ -code which is pure whenever $\text{wt}(C^{\perp_H} \setminus C) = d^{\perp_H}$.

The CSS construction extends to the AQECCs derived from Hermitian codes. We can use either the Euclidean or the Hermitian inner product if $q = e^2$ since, over \mathbb{F}_{q^2} , C^{\perp_E} and C^{\perp_H} share the same MacWilliams transform, making $d^{\perp_E} = d^{\perp_H}$.

Lemma 2.11: [11, Lem. 3.1] Let C_i be an $[n, k_i, d_i]_{q^2}$ -code for $i = 1, 2$. Let $C_1^{\perp*} \subseteq C_2$. Let $d_z := \max\{\text{wt}(C_2 \setminus C_1^{\perp*}), \text{wt}(C_1 \setminus C_2^{\perp*})\}$ and $d_x := \min\{\text{wt}(C_2 \setminus C_1^{\perp*}), \text{wt}(C_1 \setminus C_2^{\perp*})\}$. Then there exists an asymmetric quantum code Q with parameters $[[n, k_1 + k_2 - n, d_z/d_x]]_{q^2}$. The code Q is pure whenever $\{d_z, d_x\} = \{d_1, d_2\}$. If we have $C \subseteq C^{\perp*}$ where C is an $[n, k, d]_{q^2}$ -code, then Q is an $[[n, n - 2k, d'/d']]_{q^2}$ -code where $d' = \text{wt}(C^{\perp*} \setminus C)$. The code Q is pure whenever $d' = d^{\perp*}$.

III. QUANTUM CODES FROM HERMITIAN CURVE

We apply Lemmas 2.10 and 2.11 to construct quantum codes. We restrict our attention to the range where two-point codes improve on one-point codes as given in Proposition 2.5.

First we use the CSS construction with C_1 and $C_2^{\perp_E}$ in the range of improvement. This construction produces long quantum codes with excellent parameters.

Proposition 3.1: Let $0 \leq r_1 \leq r_2 \leq q(q+1)$. For $q \geq 4$, there exists a pure AQECC with parameters $[[q^3 - 1, q^3 - q(q-1) - (r_1 + r_2) + 1, d(r_2)/d(r_1)]]_{q^2}$ where $d(r_1)$ and $d(r_2)$ are computed according to Corollary 2.6.

Proof: Apply Lemma 2.11 with $C_1 = C_L(D, (q^3 - r_1 + 1 - (q+1))P + (q-1)Q)$ and $C_2 = C_L(D, (q^3 - r_2 + 1)P - 2Q)$. The nestedness $C_1^{\perp_E} \subseteq C_2$ is guaranteed by Corollary 2.3, given the range $r_i \leq q(q+1)$. The minimum distance can be computed from Corollary 2.6 since C_1 is equivalent to a code having a divisor of the form $G = iP - 2Q$. By the Riemann-Roch Theorem, $d(C_1^{\perp_E}) = q^3 - 1 - r - (q-2)(q+1)$. If $q \geq 4$, this value is larger than $d(r_i)$ for the given range. Thus the derived quantum code is pure. ■

Let the designed distance δ be fixed. Tables I and II list down the best dimension obtainable from one-point and two-point codes based on Proposition 2.5, along with the design parameter r used in Corollary 2.6.

By Proposition 3.1, the inner and the outer codes can be independently selected to be optimal when constructing an AQECC, as long as they are within the specified range. This effectively doubles the gain when switching to two-point codes. For example, the best 16-ary AQECC with $d_z = 9$ and $d_x = 5$ we can construct is of parameters $[[63, 39, 9/5]]_{16}$ if only one-point codes are considered. Using two-point codes, the value of k increases to 42.

Lemma 2.10 states a different construction, which gives AQEEC over \mathbb{F}_q instead of \mathbb{F}_{q^2} . To use the construction we need the following result about the dual codes with respect to the Hermitian inner product. The one-point version of the proposition was proved in [10].

Proposition 3.2: A two-point code $C_L(D, iP - jQ)$ with $1 \leq j$ is Hermitian self-orthogonal if $i \leq q^2 - 2$.

δ	Dimension		r
	1-point	2-point	
5	53	55	3
7	52	53	5
9	49	50	8
11	47	48	10

TABLE I
DIMENSIONS OF ONE- AND TWO-POINT CODES ON THE HERMITIAN CURVE OVER \mathbb{F}_{16}

δ	Dimension		r	δ	Dimension		r
	1-point	2-point			1-point	2-point	
9	475	481	3	33	451	454	30
11	474	481	3	35	449	454	30
13	474	481	3	37	447	450	34
15	474	475	9	39	447	448	36
17	467	472	12	41	443	445	39
19	465	472	12	43	441	443	41
21	465	472	12	45	439	441	43
23	465	466	18	47	438	439	45
25	459	463	21	49	435	436	48
27	457	463	21	51	433	434	50
29	456	459	25	53	431	432	52
31	456	457	27	55	429	430	54

TABLE II
DIMENSIONS OF ONE- AND TWO-POINT CODES ON THE HERMITIAN CURVE OVER \mathbb{F}_{64}

Proof: It is enough to prove the theorem with $j = 1$ since $C_L(D, iP - jQ) \subseteq C_L(D, iP - Q)$. By Lemma 2.4 we know that a basis for the two-point vector space can be obtained by monomial evaluation. Codewords which are Hermitian dual to $x^a y^b(P)$ are Euclidian dual to words of the form $x^{qa} y^{qb}(P)$ which live in $C_L(D, qiP)$. Adding $-Q$ to the divisor removes only the constants and any non-constant monomial to the q -th power is also non-constant. Thus the Hermitian dual of $C_L(D, iP - Q)$ contains $C_L(D, qiP - Q)^{\perp_E}$. Under the degree assumption we can use Corollary 2.3 to show that $C_L(D, qG)$ is Euclidean self-orthogonal. Hence the original code $C_L(D, G)$ is Hermitian self-orthogonal. ■

Unfortunately, this requirement is too restrictive on the range of G . Due to the small degree of G , the dual code is outside the range of improvements given in Proposition 2.5. Thus, for this particular construction, two-point codes do not improve on one-point codes already treated in [10].

IV. IMPURE AQECCS AND COSET BOUNDS

Recent results concerning the bounds for the minimum distance produce better bounds for the cosets [3]. A particular feature of the coset bounds on the Hermitian curve is that they are non-monotonic. This lack of monotonicity can be exploited to produce excellent impure AQECCs based on the CSS construction.

Best 2-point (k, d_z, d_x)	Closest 1-point (k, d_z, d_x)	I	G_1	G_2
(1, 470, 11)	(1, 470, 10)	1	$35P + 5Q$	$35P + 6Q$
(1, 471, 10)	(1, 470, 10)	1	$34P + 5Q$	$34P + 6Q$
(2, 469, 11)	(2, 469, 10)	1	$35P + 5Q$	$35P + 7Q$
(2, 470, 10)	(1, 470, 10)	1	$34P + 5Q$	$34P + 7Q$
(2, 486, 5)	(2, 486, 4)	1	$17P + 6Q$	$17P + 8Q$
(2, 487, 4)	(2, 486, 4)	1	$16P + 6Q$	$17P + 7Q$
(3, 460, 14)	(3, 460, 12)	2	$44P + 4Q$	$44P + 7Q$
(3, 461, 13)	(3, 460, 12)	2	$43P + 4Q$	$43P + 7Q$
(3, 463, 12)	(3, 460, 12)	3	$41P + 4Q$	$43P + 5Q$
(3, 477, 7)	(3, 477, 5)	2	$26P + 5Q$	$26P + 8Q$
(3, 479, 6)	(3, 477, 5)	3	$24P + 5Q$	$26P + 6Q$
(3, 486, 4)	(2, 486, 4)	1	$16P + 6Q$	$17P + 8Q$
(4, 462, 12)	(3, 460, 12)	3	$41P + 4Q$	$43P + 6Q$
(4, 468, 9)	(4, 468, 6)	3	$35P + 4Q$	$35P + 8Q$
(4, 471, 8)	(4, 468, 6)	5	$32P + 4Q$	$35P + 5Q$
(4, 478, 6)	(3, 477, 5)	3	$24P + 5Q$	$26P + 7Q$
(5, 461, 12)	(3, 460, 12)	3	$41P + 4Q$	$43P + 7Q$
(5, 463, 10)	(5, 459, 7)	7	$40P + 3Q$	$44P + 4Q$
(5, 470, 8)	(4, 468, 6)	5	$32P + 4Q$	$35P + 6Q$
(5, 477, 6)	(5, 476, 5)	2	$24P + 5Q$	$26P + 8Q$
(6, 462, 10)	(5, 459, 7)	7	$40P + 3Q$	$44P + 5Q$
(6, 469, 8)	(6, 467, 6)	4	$32P + 4Q$	$35P + 7Q$
(7, 461, 10)	(7, 458, 7)	6	$40P + 3Q$	$44P + 6Q$
(7, 468, 8)	(6, 467, 6)	4	$32P + 4Q$	$35P + 8Q$
(8, 460, 10)	(7, 458, 7)	6	$40P + 3Q$	$44P + 7Q$
(9, 459, 10)	(7, 458, 7)	6	$40P + 3Q$	$44P + 8Q$

TABLE III
BETTER AQECCS FROM TWO-POINT CODES ON HERMITIAN
CURVES OVER \mathbb{F}_{64} . IMPROVEMENT IS MEASURED BY ADDING THE
GAIN TO THE CLOSEST ONE-POINT CODE IN ALL THREE
PARAMETERS k, d_x , AND d_z .

For the Hermitian curve over \mathbb{F}_{64} we simulated all possible pairs of two-point divisors (up to equivalence) $G_1 \leq G_2$ of degrees $0 \leq \deg G_1 \leq \deg G_2 \leq q(q-1)$ and calculated the parameters of the impure asymmetric quantum code constructed based on the nested pair $C_1 = C_\Omega(D, G_2) \subseteq C_\Omega(D, G_1) = C_2$.

An implementation of the methods for coset bounds given in [3] was used to calculate $d_z = \text{wt}(C_2 \setminus C_1)$. Note that $d_x = \text{wt}(C_1^{\perp_E} \setminus C_2^{\perp_E}) = n - \deg G_1 + 2g + 2$ since it falls in the range where it can be completely determined by the Riemann-Roch Theorem. To find the exact improvement, the parameters of the best AQECCs derivable from one-point codes, *i.e.* codes with divisors $G_1 = iP$ and $G_2 = jP$, were stored separately and then compared with the parameters of the AQECCs constructed from nested two-point codes.

Based on the computational data, we present in Table III all two-point codes which strictly improve on one-point codes. The resulting quantum codes are of parameters $[511, k, d_z/d_x]_{64}$.

REFERENCES

- [1] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3065–3072, 2001.
- [2] P. Beelen, "The order bound for general algebraic geometric codes," *Finite Fields Appl.*, vol. 13, no. 3, pp. 665–680, 2007.
- [3] I. Duursma, R. Kirov, and S. Park, "Distance bounds for algebraic geometric codes," to appear in *Journal of Pure and Applied Algebra*, 2010.
- [4] I. Duursma and R. Kirov, "Improved Two-Point Codes on Hermitian Curves", to appear in *IEEE Transactions of Information Theory*, 2011.
- [5] M. Homma and S. J. Kim, "Toward the determination of the minimum distance of two-point codes on a Hermitian curve," *Des. Codes Cryptogr.*, vol. 37, no. 1, pp. 111–132, 2005.
- [6] M. Homma and S. J. Kim, "The complete determination of the minimum distance of two-point codes on a Hermitian curve," *Des. Codes Cryptogr.*, vol. 40, no. 1, pp. 5–24, 2006.
- [7] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 52, pp. 4892–4914, 2006.
- [8] G. L. Matthews, "Weierstrass pairs and minimum distance of Goppa codes," *Des. Codes Cryptogr.*, vol. 22, no. 2, pp. 107–121, 2001.
- [9] S. Park, "Minimum distance of Hermitian two-point codes," *Designs, Codes and Cryptography*, vol. 57, no. 2, pp. 195–213, 2010.
- [10] P. K. Sarvepalli and A. Klappenecker, "Nonbinary quantum codes from Hermitian curves," *Applied algebra, algebraic algorithms and error-correcting codes*, 136–143, Lecture Notes in Comput. Sci., 3857, Springer, Berlin, 2006.
- [11] P. K. Sarvepalli, A. Klappenecker, and M. Rötteler, "Asymmetric quantum codes: constructions, bounds and performance," *Proc. of the Royal Soc. A (2009)*, vol. 465, pp. 1645–1672, 4 March 2009.
- [12] H. Stichtenoth, "A note on Hermitian codes over $\text{GF}(q^2)$," *IEEE Trans. Inform. Theory*, vol. 34, no. 5, part 2, pp. 1345–1348, 1988. Coding techniques and coding theory.
- [13] H. Stichtenoth, *Algebraic function fields and codes*, vol. 254 of *Graduate Texts in Mathematics*. Berlin: Springer-Verlag, second ed., 2009.
- [14] H. J. Tiersma, "Remarks on codes from Hermitian curves," *IEEE Trans. Inform. Theory*, vol. 33, no. 4, pp. 605–609, 1987.
- [15] M. Tsfasman, S. Vlăduț, and D. Nogin, *Algebraic geometric codes: basic notions*, vol. 139 of *Mathematical Surveys and Monographs*. Providence, RI: American Mathematical Society, 2007.
- [16] L. Wang, K. Feng, S. Ling, and C. Xing, "Asymmetric quantum codes: characterization and constructions," *IEEE Trans. Inform. Theory*, vol. 56, pp. 2938–2945, 2010.